Sécurité 2

Université Kasdi Merbah Ouargla

Département d'Informatique et des Technologies de l'Information

ETUDE DES ATTAQUES

Classification des attaques

2 ème Année Master RCS

Septembre 2014

Plan du cours

1. Classification des attaques

- Ecoute passive
- Interception
- Déguisement
- Cryptanalyse
- Déni de service
- Bombe logique
- Porte dérobée
- cheval de Troie
- RootKits
- Spyware
- Spamming
- Virus
- Vers
- Débordement de tampon (buffer overflow)

Plan du cours

Remarque : slides basés sur les cours de sécurité d'Anas ABOU EL KALAM

1. Classification des attaques

- Ecoute passive
  - l'attaquant se contente d'accéder sans modification aux informations générées (e.g., sur un Disque Dur), transmises sur un canal de communication.

  $\Rightarrow$ sniffing, scanning, eavesdropping, wire tapping

- Interception
  - l'attaquant modifie des informations transmises ou injecte des informations

  $\Rightarrow$ rejeu, insertion, substitution, destruction, vol de session TCP (TCP hijacking)

- Déguisement
  - l'attaquant tente de se faire passer pour quelqu'un d'autre

  =>IP spoofing, web page defacing, Fishing

- Cryptanalyse
  - obtenir des informations secrètes a partir d'informations publiques

  => a partir d'un message chiffré, retrouver le message en clair, retrouver la clé

Classification des attaques

- **Déni de service**

  l'attaquant vise à empêcher sa victime de continuer à délivrer le service (attaque de la disponibilité)

  ⇒spamming, flooding, smurfing

- **Bombe logique**

  sont aussi néfastes que les virus ou les vers et sont la cause de dégâts similaires. La différence est que la bombe logique a besoin d'un détonateur pour s'activer,

  C'est donc une fonction destructive (partie de programme qui reste dormante) déclenchée à retardement ou par certaines conditions :

  - ✓ date précise (vendredi 13)
  - ✓ présence de certains utilisateurs, certains logiciels ou matériels
  - ✓ après un certain nombre d'activations

  => destruction d'infos stockées : données, pgms, infos de sécurité (ex: par formatage Disque Dur)

  => diffusion de fausses informations de diagnostic

  => dégâts matériels : usure anormale de périphériques, destruction d'écrans, de disquettes, d'imprimantes, etc.

Classification des attaques

Porte dérobée (Backdoors)

- Accès cachés, moyen de contourner les mécanismes de sécurité
- faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle (cheval de Troie en particulier)
- Ces passages secrets sont ménagés par les concepteurs de logiciels pour fournir des accès privilégiés pour les tests ou la maintenance.
  - Mais les pirates qui les découvrent peuvent déjouer tous les mécanismes de sécurité et rentrer dans le système.
- Parfois installée par un attaquant qui a réussi à s'introduire dans le système et qui veut se laisser un moyen de se réintroduire dans le système

exemple :

- août 1986, Lawrence Berkeley Laboratory : un intrus utilise le compte d'un utilisateur puis acquiert les privilèges systèmes : faille banale (mauvaise installation de Gnu-emacs)
- plutôt que de corriger la faille, il est décidé d'observer
- en 10 mois, l'intrus a tenté de pénétrer dans 430 ordinateurs reliés à Internet, principalement militaires
- il a été possible de localiser et d'identifier l'intrus : un allemand de Hanovre, Markus Hess, lié au Chaos Computer Club et travaillant pour le KGB (condamné le 15 février 1990 à des peines de 2 ans de prison avec sursis et de 10 000 DM d'amende)

Classification des attaques

Porte dérobée (Backdoors)

- Ex de backdoors sur certains logiciels (messagerie, utilitaires systèmes)
  - e.g., pour certaines commandes suivies d'arguments particuliers ou avec un mot de passe bien défini, le logiciel peut avoir un comportement différent
    - Permettre accès root à l'utilisateur, renvoyer un shell système à l'utilisateur, etc.
- Ces "trappes" sont inclues directement dans le code du logiciel.
- Certains développeurs sont soucieux de posséder un accès sur tous les systèmes utilisant leurs logiciels !!
  - e.g., Ken Thompson, l'un des pères d'UNIX, avoue avoir modifié l'application /bin/login en permettant l'accès direct au système par la saisie d'un mot de passe précompilé en dur. Thompson pouvait ainsi visiter tous les systèmes utilisant son application modifiée.
- Parfois, certains pirates diffusent des applications infestées de backdoors

Classification des attaques

Comment se protéger contre les portes dérobées?

- ✓ MAC & Checksums & Signatures
- ✓ Veille : CERT, BugTraq, ...
- ✓ Télécharger les applications sur le site du distributeur ou du programmeur.
  - Utiliser des serveurs de téléchargement non liés à l'auteur de l'application peut se relever dangereux.

Classification des attaques

- cheval de Troie
  - ❖ programme effectuant une fonction illicite tout en donnant l'apparence d'effectuer une fonction légitime ;
  - ❖ la fonction illicite peut être de divulguer ou d'altérer des informations, ou peut être une bombe logique

Exemple AIDS

entre le 8 et le 12 décembre 1989, environ 10.000 disquettes "publicitaires" ont été envoyées à 7000 abonnés de PC Business World (GB) et à 3000 participants européens d'une conférence de l'OMS sur le SIDA en octobre 1988.

- l'enveloppe contenait : le texte d'une licence et le mode d'emploi d'installation
- objet prétendu du programme : évaluer le risque d'être atteint par le SIDA
- en fait, après 90 démarrages du PC, une bombe logique était lancée :
  - chiffrement des noms de fichiers sur le disque
  - édition d'un bon de commande pour payer la licence à l'ordre de PC-Cybor

Protection ?

- ✓ Antivirus,
- ✓ MAC & Signatures
- ✓ Veille : CERT, BugTraq, ...
- ✓ Ne pas faire confiance aux pgms non sûrs, Macros, ...

Classification des attaques

- RootKits
  - ❖ programme permettant d'automatiser la dissimulation et l'effacement des traces d'un pirate sur une machine.
  - ❖ Modifier commandes permettant d'administrer système, cacher ports ouverts par pirate...
  - ❖ Utilisent le principe des backdoors
  - ❖ ++ types : ls, ps, netstat ==>Modif lib ==> Modif comportement noyau, par le biais de modules chargés en mémoire

Protection ?

Les checksums.

- ✓ effectuer checksums à la fin d'une installation sur les différents fichiers comme ls, ps, netstat, ifconfig, etc. et sur les différentes bibliothèques partagées.
- ✓ Cette version d'OS devrait être stockée sur CDROM ou autre support non réinscriptible.

Compiler les programmes vitaux en statique.

- ✓ disposerez d'une trousse de secours en cas d'infection par rootkits.
- ✓ pour cela, il faut disposer d'un OS permettant accéder sources pgms vitaux...

Chkrootkit permet de détecter la présence d'un rootkit (sous FreeBsd, libre).

Compilez noyau en statique. Vous éviterez ainsi chargement modules externes.

Classification des attaques

- Spyware

  contraction de spy et software.

  Logiciel espion qui collecte des données personnelles avant de les envoyer à un tiers,

  e.g., Keylogger : transmettre les données saisies au clavier

- Spamming

  l'usage abusif d'un système messagerie destiné à exposer délibérément (et de manière répétée) les utilisateurs à des contenus non pertinents et non sollicités

Classification des attaques

- virus

- segment de programme qui, lorsqu'il s'exécute, se reproduit en s'adjoignant à un autre programme (du système ou d'application), et qui devient ainsi un cheval de Troie ;
- Propriétés : infection, multiplication, fonction nocive

  => éventuellement porteur d'une bombe logique

  $\Rightarrow$propagation par échange de support (flash disk) ou par réseau
- peut simplement s'adjoindre à un autre programme et être donc exécuté uniquement lorsque ce programme est exécuté
- peut s'installer dans le secteur de boot d'une machine, d'une disquette ou dans la table des interruptions : on parle de *virus résident*

Classification des attaques

macros-virus

- dans certains documents, des commandes peuvent être enregistrées comme des données (formules de calcul dans les tableurs ou macros dans des traitements de texte)
- ces commandes peuvent être exécutées à l'ouverture du fichier

  => un virus peut s'insérer dans ces commandes

  => un logiciel comme Excel prévient de la présence de telles macros et demande l'autorisation pour les exécuter

virus de messagerie

- un cheval de Troie est inséré dans un document attaché à un courrier électronique
- tout est fait pour que l'utilisateur exécute le document attaché (titre trompeur, ...)

Classification des attaques

- Virus "vendredi13" (Israël, décembre 1987) :
  - virus pour PC, avec une bombe logique
  - détruit les programmes lorsqu'il s'exécute un vendredi 13
- virus "nimda" (septembre 2001) :
  - virus pour PC, contenant un cheval de Troie;
  - ce virus se répand par fichiers attachés dans la messagerie
  - pas de sujet, document attaché « README.EXE »
  - le virus peut s'exécuter automatiquement à l'ouverture du mail sous Outlook
  - il provoque le partage en écriture du disque local
  - il tente de se propager par les dossiers partagés
  - il tente de saturer les serveurs de messageries et scane massivement le port 80 de certains serveurs web pour dégrader leurs performances
- virus "Iloveyou" (2000) :
  - virus de messagerie électronique
  - le sujet est « I love you »
  - un document attaché LOVE-LETTER-FOR-YOU.TXT.vbs contient un virus
  - détruit beaucoup de fichiers locaux en les remplaçant par sa propre copie,
  - essaie également de se propager par messagerie et par IRC (chat sur intenet)

Classification des attaques

- Vers

- programme autonome qui s'exécute, se propage et se reproduit à L'insu des utilisateurs normaux

  => éventuellement porteur d'une bombe logique

  => propagation par réseau

- premier ver, Xerox, 1975 : programme "utile", composé de segments qui se copiaient sur les machines inactives du réseau (tests de machines, mesure de performances ...)

- le ver d'Internet (2 novembre 1988) :

  créé par Robert Morris Jr., étudiant, fils de Robert H. Morris ("Chief Scientist" du «National Computer Security Center » de la National Security Agency)

  utilise 3 failles connues d'Unix dont l'attaque par dictionnaire des mots de passe

  suite à une faute de conception, le ver se propage beaucoup plus rapidement que prévu par son auteur (condamné à 10 000 $ d'amende et 400 heures de travaux d'intérêt général)

  => immobilisation de 6000 à 60000 machines en une nuit

  => création du Computer Emergency Response Team (CERT) le 13 décembre

Classification des attaques

- Vers suite

➢ "Blaster" (connu également sous le nom de "Lovsan") :

– infecte les machines WindowsNT, Windows2000, Windows XP et Windows Server 2003

– exploite une faiblesse de DCOM (Distributed Component Object Model) qui utilise le port TCP/IP 135

⇒ suffit d'envoyer une requête particulièrement formatée pour provoquer une défaillance (buffer overflow)

– un email contenant un cheval de Troie a ensuite circulé en prétendant contenir un correctif pour le vers !

=> les correctifs de sécurité ne sont en général jamais envoyés par courrier !!

– modification de la base des registres

– génération d'une adresse IP et tentative d'infection de la machine correspondante

– création d'un processus qui écoute sur le port 1444 et qui permet d'exécuter à distance des commandes sur la machine infectée

– en fonction de certaines conditions (certains jours de certains mois), une attaque de type déni de service est lancée contre le site windowsupdate.com (SYN flooding)

Définitions :

Ver	Virus
Autonome sur DD (n'utilise pas nécessairement un fichier pour se propager),	Parasite dissimulé dans fichiers ou dans code exécutable contenu dans secteur démarrage disque
Arrive souvent par pièce jointe à un mail comprenant un code malicieux exécuté automatiquement par le logiciel de courrier électronique ou manuellement par l'utilisateur	Souvent par port réseau
ne se multiplie pas localement	se multiplie localement, s'autoduplique, se propage en infectant tour à tour les fichiers Effets : fichiers effacés, disque dur formaté, saturation des disques, modification du MBR

Classification des attaques

- **Buffer overflow**

- attaque qui n'utilise pas une faiblesse du réseau mais très utilisée pour attaquer les réseaux

  => consiste à exploiter des faiblesses des programmes serveurs qui s'occupent de services réseaux (serveur ftp, serveur http, ...)

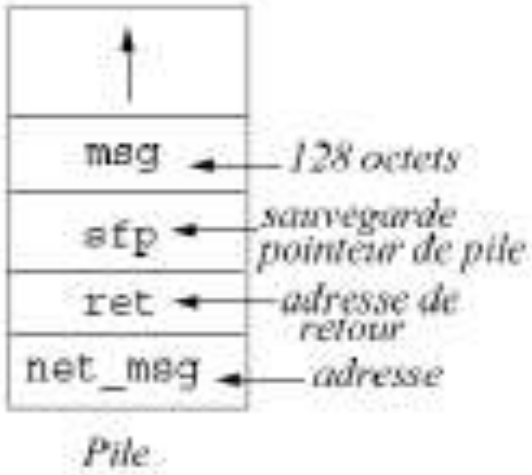
- le principe : exploiter des bugs dans des programmes C!

```
void copy_msg(char * net_msg)

msg[128];

strcpy(msg,net_msg);
return;
```

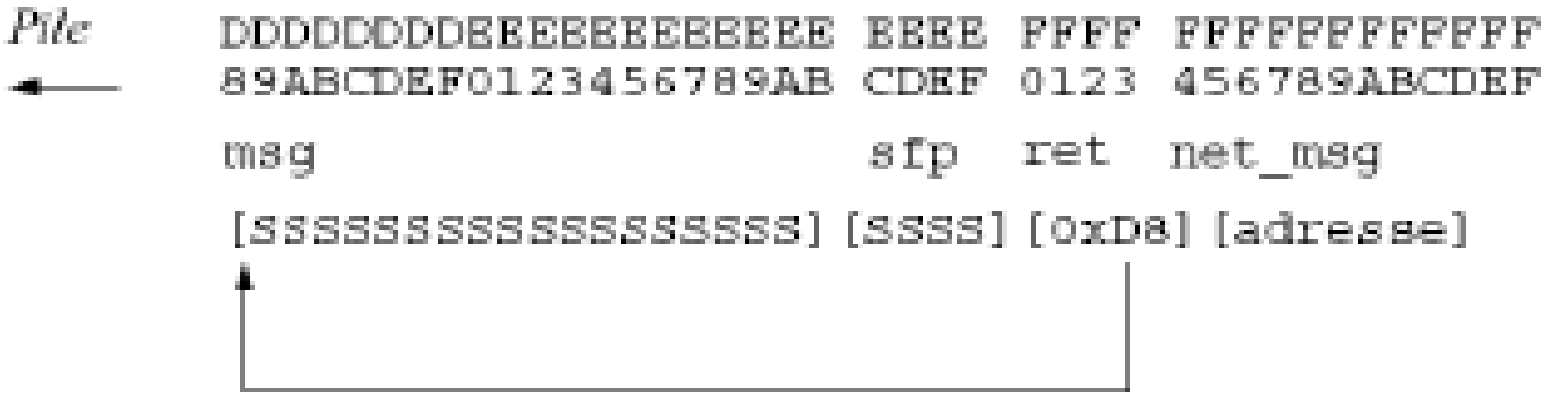
copie de `net_msg` *dans* `msg`
sans vérifier la taille de `net_msg`



Classification des attaques

- **Buffer overflow**

- si net_msg est trés long , il peut écraser msg puis sfp puis l'adresse de retour de la fonction copy_msg (ce qui n'est pas normal !)
- lorsque la fonction copy_msg se termine, on peut alors faire exécuter du code à une adresse choisie => justement celle de msg
- le code à exécuter est inséré dans net_msg qui est donc copié dans msg



=> ici le code à exécuter est : SSSSSSS..... S

=> l'adresse de retour a été changée en 0xD8, à l'endroit où a été placé le code à exécuter

=> l'art consiste donc à fabriquer net_msg = SSSS.....SS0xD8

Classification des attaques

- Buffer overflow : example «Buffer overflow de wu-ftpd par MAIL_ADMI»

- Lorsque la fonctionnalité MAIL_ADMIN de wu-ftpd est activée, un attaquant distant pourrait provoquer un débordement de mémoire.
- Le serveur wu-ftpd peut être compilé avec la fonctionnalité MAIL_ADMIN. Dans ce cas, un email est envoyé vers administrateur chaque fois qu'un fichier est uploadé sur le serveur.

  From: wu-ftpd

  Subject: New file uploaded: nom_fichier
- Cependant, si la taille du nom de fichier avoisine les 32768 caractères, *un buffer overflow* se produit.
- Un attaquant pourrait donc employer cette vulnérabilité dans le but de faire exécuter du code.

Classification des attaques

- Buffer overflow : example « Buffer overflow de ipcs »

- Le programme /usr/bin/ipcs fournit des informations sur l'usage des ressources IPC (Inter Process Communication).
  - ipcs affiche le nombre de queues de message et de sémaphores créés ainsi que les segments de mémoire.
- L'option "-C" indique la source d'informations à employer. En général, il s'agit d'un fichier core. Par exemple :
  - **ipcs -C /tmp/core**
- Cependant, ipcs ne vérifie pas la taille du nom de fichier !!
- Un attaquant local peut alors spécifier un nom de fichier core trop long dans le but de provoquer un buffer overflow.
- e.g., permettre à un attaquant local d'accroître ses privilèges.